



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/067,610	02/04/2002	Rafie Shamsaasef	70670	5884

22242 7590 10/11/2005

FITCH EVEN TABIN AND FLANNERY
120 SOUTH LA SALLE STREET
SUITE 1600
CHICAGO, IL 60603-3406

EXAMINER

OKORONKWO, CHINWENDU C

ART UNIT PAPER NUMBER

2136

DATE MAILED: 10/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/067,610

Applicant(s)

SHAMSAASEF ET AL.

Examiner

Chinwendu C. Okoronkwo

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 February 2002.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 20020204.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

AT

DETAILED ACTION

1. Pursuant to USC 131, claims 1-20 are presented for examination.
2. Claims 1-20 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being disclosed by (U.S. Patent Publication No. 20030093694).

Regarding claim 1, Medvinsky et al., discloses a communication authorization method, comprising the steps of:

- receiving a request for access information to access content (0015);
- generating the access information to access the desired content from a first application server (0015);
- generating authentication of the access information using a first service ticket (0016); and
- sending the access information and authentication to a client (0015 and 0016).

Regarding claim 2, Medvinsky et al., discloses the method as claimed in claim 1, wherein the step of generating authentication including generating a third party server signature using the first service ticket, wherein the first service ticket is a third party server service ticket to the first application server (0059).

[*The examiner's reasoning:* Applicant describes a service ticket as being equivalent or analogous to session key, which is analogous to a public key. Therefore the rejection is made on the basis that the certificate disclosed by Medvinsky et al. is the central unit (third party server) signature using the public key (service ticket).]

Regarding claim 3, Medvinsky et al., discloses the method as claimed in claim 1, wherein the step of generating the access information including generating session rights and encrypting at least a portion of the session rights using a third party server service key for

the first application server (0017, 0035 and 0037).

[*The examiner's reasoning:* The "ticket" disclosed by Medvinsky et al. (0037 of Medvinsky et al.) comprising "client authorization data" which is analogous to the claimed session rights. The same ticket, or at least the content(s), is encrypted with a "service key" (0035 of Medvinsky et al.).]

Regarding claim 4, Medvinsky et al., discloses the method as claimed in claim 1, further comprising the step of: encrypting at least a portion of the authentication using the first service ticket (0035 and 0036).

Regarding claim 5, Medvinsky et al., discloses the method as claimed in claim 4, further comprising the steps of:

- requesting a ticket granting ticket (TGT ticket) (0041);
- receiving a TGT ticket (0042);
- requesting the third party server service ticket for the first application server (0039 and 0053); and
- receiving the third party server service ticket for the first application server (0039 and 0054).

[*The examiner's reasoning:* The claimed "service ticket" is analogous in function to "caching server ticket" disclosed by Medvinsky et al..]

Regarding claim 6, Medvinsky et al., the method as claimed in claim 1, further comprising the steps of:

- receiving a key request including the access information and authentication (0047);
- extracting the access information and authentication (0047 and 0048);
- verifying the authentication of the access information using the first service ticket, and client authorization (0048); and
- issuing a key reply if the authentication of the access information and client authorization are verified (0048).

Regarding claim 7, Medvinsky et al., the method as claimed in claim 6, further comprising the steps of:

- a client generating a key request including the access information and the authentication (0047 and 0137);
- sending the key request to the first application server (0047 and 0137); and
- receiving the key reply (KEY_REP) if the authentication of the access information and client authorization are verified by the first application server (0048 and 0047).

Regarding claim 8, Medvinsky et al., discloses a method for verifying authorization for a client to gain access to content and/or services, comprising the steps of:

- receiving a key request (0047);
- extracting third party server access information and third party server authentication from the key request (0047 and 0048);
- verifying an authentication of the third party access information and a client authorization (0048); and
- issuing a key reply if the authentication of the third party access information and the client authorization are verified (0048).

Regarding claim 9, Medvinsky et al., discloses the method as claimed in claim 8, further comprising the step of authenticating the third party server access information using the third party server authentication (0017 and 0035).

Regarding claim 10, Medvinsky et al., discloses the method as claimed in claim 9, wherein the step of authenticating includes extracting a first service ticket from the authentication and authenticating the third party server access information using the first service ticket (0017, 0035, 0037, 0047 and 0048).

Regarding claim 11, Medvinsky et al., discloses the method as claimed in claim 8, wherein the step of extracting the third party server authentication, further comprising:

- the steps of extracting a session key from the key request (0048); and
- the step of authenticating the access information including verifying a third party server signature using the session key (0035).

Regarding claim 12, Medvinsky et al., discloses the method as claimed in claim 11, wherein the step of extracting the session key including decrypting at least a portion of the key request using an application server service key and extracting the session key (0048 and 0143).

[*The examiner's reasoning:* The disclosure by Medvinsky et al. states that the DOI object data is a portion of the disclosed "caching server ticket" (analogous to the claimed "session key") and "may be encrypted." Decryption is thus implied when Medvinsky et al. discloses the extracting of the DOI object.]

Regarding claim 13, Medvinsky et al., discloses the method as claimed in claim 8, further comprising the steps of:

- receiving a request for the access information to access content (0015);
- generating the third party server access information to access the desired content from a first application server (0015); and
- generating the third party server authentication of the access information (0016).

Regarding claim 14, Medvinsky et al., discloses the method as claimed in claim 13, wherein the step of generating the third party server authentication including incorporating a third party server service ticket for the first application server (0059).

Regarding claim 15, Medvinsky et al., discloses the method as claimed in claim 14, wherein the step of generating the authentication including generating a signature utilizing a session key of the third party server service ticket (0016).

Regarding claim 16, Medvinsky et al., discloses the method as claimed in claim 14, wherein the steps of verifying the authentication of the access information including extracting the third party server service ticket and verifying the third party server service ticket (0017 and 0035).

Regarding claim 17, Medvinsky et al., discloses a method for providing secure communication when distributing services, comprising: the steps of:

- receiving a selection for services (0015);
- issuing access information for the services (0015);
- issuing authentication of the access information (0016);
- receiving a key request (0047);
- verifying an authentication of the access information and a client authorization utilizing, at least in part, a first service ticket (0048); and
- issuing a key reply to a client if the authentication of the access information and the client authorization are verified (0048).

Regarding claim 18, Medvinsky et al., discloses the method as claimed in claim 17, further comprising the steps of:

- receiving a first service ticket request from a third party server for a first server (0137 and 0141);
- issuing the first service ticket to the third party server for the first server (0085); and
- the steps of issuing access information and authentication including generating the access information and authentication using the first service ticket (0015 and 0016).

Regarding claim 19, Medvinsky et al., discloses the method as claimed in claim 17, further comprising the steps of:

- receiving a second service ticket request for the first server (claim 20);
- issuing a second service ticket for the first server (claim 20); and
- the step of receiving a key request wherein the key request includes the second service ticket (claim 20).

[*The examiner's reasoning:* Because Medvinsky et al. discloses the user (client server) being allowed "to stream the content from the caching server," it is understood that the second service ticket **must first** be issued.]

Regarding claim 20, Medvinsky et al., discloses the method as claimed in claim 17, wherein: the step of verifying the authentication of the access information including:

- extracting the first service ticket (0047 and 0048);

Art Unit: 2136

- decrypting the first service ticket (0036);
- extracting a session key from the first service ticket (0048 and 0036);
- generating a signature using the session key (0059); and
- verifying the signature with the authentication (0048).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses key management and exchange protocols.

U.S. Patent Publication: U.S. 2003/0059053 A1 – Medvinsky et al.

U.S. Patent: 6,775,772 B1 – Binding et al.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 7:15 - 4:30 and TuTh 8:00 - 4:30.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272 3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



CCO



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100